A New Analytical Model of Shared Backup Path Provisioning in GMPLS Networks

SuKyoung Lee, David Griffith and Nah-Oak Song

National Institute of Standards and Technology

100 Bureau Drive, Stop 8920, Gaithersburg, MD 20899

Abstract

As GMPLS and its supporting set of protocols develop into a viable control plane for optical networks, an important function that they will need to support will be the protection and restoration function that has been a major feature of legacy optical networks. A network with a robust set of protection and restoration mechanisms will be able to support data traffic while allowing faster recovery from failures than can be obtained using layer 3 rerouting. Several models have been proposed for protection with GMPLS using shared backup paths. This previous work has not investigated the effect on recovery time critical to the service or the number of backup paths that are required to meet a desired level of performance. Using both restoration time and recovery blocking probability, we have developed a new analytic model for GMPLS-based recovery in $M : N$ protection groups. Furthermore, we show that smaller backup paths can be reserved by capturing the effect of multiple failures in the case of $M : N$ shared protection with revertive mode in an optical network with a GMPLS control plane.

Keywords: GMPLS, Shared Backup Path, Multiple failures

I Introduction

Protection of traffic is growing in importance and especially recovery schemes that can provide fast restoration at layers above the optical layer. MPLS-based recovery has been pointed out as strong candidate in this area and may be motivated by the notion that there are inherent limitations to improving the recovery times of current routing algorithms. Since GMPLS is likely to be the technology of choice in the future IP-based transport network, it is necessary that MPLS be able to provide protection and restoration of traffic. Furthermore, a protection mechanism using GMPLS could enable IP traffic to be put directly over WDM optical channels, without an intervening SONET layer, while still emulating SONET resiliency features. This would facilitate the construction of IP-over-WDM networks. For restoration in IP over WDM network, even if link-layer restoration such as mesh

restoration is recommended to achieve low latencies, IP level restoration, based on GMPLS recovery is employed in the event that link-layer restoration fails.

It is generally desirable to have protection and restoration schemes that are bandwidth efficient. In GMPLS-based recovery, it is important to increase network reliability by providing necessary resources in time as well as enabling a fast response to faults. In this paper, a new backup path provisioning scheme is proposed in order to reflect this tradeoff between resource utilization and reliability upon GMPLS-based recovery.

There have been many proposals in the IETF (Internet Engineering Task Force) to standardize methods of signaling and provisioning GMPLS networks to achieve protection against failures. However, to support the routing of backup paths for $M : N$ path protection, new extensions must be added to the current GMPLS routing extensions. In particular, there must be a mechanism to advertise backup path bandwidth and processing rules must be defined for bandwidth accounting when backup path requests arrive at a node. Therefore, we investigate an analytic model of restoration time in the case of $M : N$ shared protection. Also, we analyze the restoration request failure probability numerically for the case that multiple failures occur upon a path in $M : N$ protection with revertive mode. Furthermore, in our scheme, a protection priority could be used as a differentiating mechanism for premium services that require high reliability. That is, guaranteed services could be provided in terms of continuity of services maintained by GMPLS-based recovery around network failures.

II GMPLS Signaling and QoS Support

The main objective of any recovery scheme is to operate in a cost-effective manner while minimizing service interruptions to the customer. Providing a high degree of reliability (or equivalently, a low probability of service disruptions) is expensive and tends not to scale well. For this reason, any carrier that operates a wide-area optical backbone network needs to be able to support a variety of service classes in which the degree of protection is tied to the price of the service [1]. For instance, [2] proposed a multi-tiered service model in which the basic (least expensive) service receives no protection support, while more expensive service options feature some various combinations of routing around areas with a relatively high probability of network failure and dedicating backup paths for automatic failover switching of the data stream.

There are mainly two levels of recovery mechanisms: rerouting and protection switching. While rerouting is defined as the real-time establishment of appropriate resources to recover affected traffic, protection switching involves the establishment of pre-calculated replacement resources. In the latter scheme, the pre-calculated backup paths can be either shared or dedicated:

- $1 + 1$: As dedicated facility recovery, traffic is passing through both the working and backup paths. Upon failure detection, the traffic on the backup path becomes the active traffic. Therefore, the resources on both the backup and the working paths are fully reserved. It is the fastest protection switched recovery mechanism, but also the most expensive in terms of resources.

- $1:N$: As semi-dedicated facility recovery, N working paths are protected using a backup path. the traffic is rerouted to the spare resource after the failure has occurred. $1:1$ protection is a special case of $1:N$ protection.

- $M:N$: As shared facility restoration, M protection entities are shared among N working resources. The most common notion $M:N$ path protection is to route N node-disjoint primary paths and pre-establish M backup paths that are node disjoint from the primary paths.

In this paper, we concentrate on the $M:N$ shared path protection method. Using GMPLS signaling [3], this method is done by indicating the LSP (Label Switched Path) is of type Secondary in the protection field of the Generalized Label Request. Backup LSPs are used for fast switchover when primary LSPs fail. Although the resources for the backup LSPs are pre-allocated, lower priority traffic may use the resources with the caveat that the lower priority traffic will be preempted if the primary LSP fails. If lower priority traffic is using resources along the secondary LSPs, the end nodes may need to be notified of the failure in order to complete the switchover. Therefore, even if the backup path is pre-signaled, it takes time to switch the traffic to the backup path allowing preemption. Actually, in a differentiated services scenario, the need for preemption becomes more compelling. Moreover, in the emerging optical internetworking architectures, where some protection and restoration functions may be migrated from the optical layer to data network elements such as gigabit and terabit LSRs (label switching routers) to reduce costs, preemptive strategies can be used to reduce the possible chances of rerouting for high priority traffic trunks under failure conditions.

GMPLS introduces a new Notify message to the signaling protocols so that LSP failures can be reported to the ingress or some other node responsible for error recovery. The setup of the primary LSP should indicate that the LSP initiator and terminator wish to receive Notify messages using the Notify Request object (RSVP Notify message) [4]. Upon receipt of the Notify messages, the source and destination nodes switch the traffic from the primary LSP to the backup path. Notify messages may provide faster error reporting than the normal error notifications since they can contain information about multiple failed LSPs, and because they are sent direct to the consumer. Note that this function is initially only specified for RSVP-TE signaling and not CR-LDP. The Protection Object is also proposed to indicate specific protection attributes of an LSP [4, 5].

Moreover, for protection, backup path management and proper management of bandwidth on the backup path is necessary. In our scheme, the management system would control each path differently in accordance with its service class maintaining the different protection resource pools. Especially, the recovery manager needs to ensure that the amount of protection resources designed for each path belonging to higher priority service is sufficient for the traffic to be protected within this service class. The priorities may be implemented for allocating shared resources under multiple failure case.

Protection bandwidth capacity could be considered as the main cost of recovery QoS. Under multiple failure case, more than one connection can claim shared resources. Thus, it is possible that a protection path may

not be successfully activated when multiple and concurrent failure events occur. In this case, shared protection bandwidth capacity may be requested by more than one failed connection and the protection path can be activated only for some of them. In order to support all the connections with the failures, enough capacity can be reserved in advance. However, this reservation will result in wasting the resources in network. Therefore, it is desirable to support priority based allocation of shared resources during restoration signaling. In the proposed scheme, the protection manager allocates different capacity in accordance with the restoration failure probability, i.e. restorability requested by each service class. The class with higher priority such as real-time traffic ought to request lower restorability.

To differentiate the protection level of each path, the field Service Type (8 bits) in Generalized Label Request can be used. Similar to Service Type defined in [6], this field indicates a class of service. Thus, a carrier may specify a range of different classes of service (e.g. gold, silver, bronze) with different types of recovery plans where there could exist no recovery, 1+1 protection, shared protection and etc. as can be seen the protection level example in Table 1.

III Backup Path Provisioning

In protection, network can quickly utilize pre-provisioned backup resources for recovery from a resource failure along the working (primary) path. That is, backup path can be setup simultaneously with the primary path to guarantee fast switching to the protection path. In accordance with the level of recovery guarantee, the resources along the backup path can be exclusively deployed (dedicated path), or they can be shared among multiple backup paths. Meanwhile, at the time when the fault occurs, the network state is not static, i.e. the number of occupied backup paths and the number of faults are different. Actually, some amount of protocol signaling is required at the time of failure. This varies from simply propagating the error from the point of detection to the point of recovery, to the full signaling of the backup path. Thus, it is usually difficult to predict how much backup paths will be necessary for the shared backup path case. In spite of this difficulty, it is not desirable to use real-time (e.g. rerouting) approach for some high priority services since the approach requires time to compute the alternate path after failure is detected and hence is likely to be slower. In consideration of the tradeoff among restoration time and pre-provisioned resource, we will analyze the restoration time to provision the shared backup path efficiently before a failure happens.

In this section, we investigate the number of enough backup paths to recover the data on the working paths based on a model for the recovery signaling time. The number of attempts depends on current network status. (e.g. how many backup paths are used and if the resources are available in the backup path.)

III-A Restoration Time Analysis

The time taken from the instant a link fails to the instant the backup path of a connection traversing the failed path is enabled, could be defined to be the protection-switching time for the connection. Our restoration time

analysis concentrates on this protection-switching time. As soon as a failure is detected on a working path, an attempt will be made to restore the working path. We assume that the control network is reliable, i.e., does not incur message losses.

Assume that there is an infinite number of feasible backup paths $\{P_1, P_2, \ldots\}$ for attempts. The backup paths will be attempted in the order numbered until the restoration is successfully made. For the i^{th} attempt to a backup path P_i, it take time t_i to check if the path P_i is available for the restoration. And assume that these times $t_1, t_2, \ldots$ are independent and identically distributed (i.i.d.) random variables having a distribution $F_t(t)$.

Let a path with a failure need K attempts until the restoration is successfully made. That is, the first $K-1$ attempts find that the paths $P_1, P_2, \cdots P_{K-1}$ are not available but the K^{th} attempt finds that the path P_K is available for restoration. Then the restoration time T_r, which is required for finding an available path to restore a working path with failure, is

$$T_r = t_1 + t_2 + \cdots + t_K \qquad K \geq 1 \tag{1}$$

It is also assumed that each attempt is successful with probability p, that is, each backup path is available for restoration with probability p. Thus, the expected number of attempts that will be required to activate a backup path is

$$\begin{aligned} E[K] &= p + 2(1-p)p + 3(1-p)^2 p + \cdots \\ &= \sum_{K=1}^{\infty} K(1-p)^{K-1} p \\ &= \frac{1}{p}. \end{aligned} \tag{2}$$

Since $t_1, t_2, \cdots$ are i.i.d. random variables with finite expected values and K is a stopping time for $t_1, t_2, \cdots$, we can apply renewal theory to Eq. 1. Then, we have

$$E[T_r] = E[K]E[t], \tag{3}$$

where $E[t] = \int_0^\infty t \, dF_t(t)$. For the case where t_K is exponentially distributed with mean $1/\mu$, $E[T_r]$ becomes $\frac{1}{p\mu}$.

Each traffic flow will have its own expected restoration time limit. The network QoS manager could use the result from Eq. 3 as a constraint on the requested restoration time. The average restoration time is indicative of the expected amount of data lost during a failure. That is, during the time required to activate the backup path and switch the traffic over to it, the affected connection will experience data (and revenue) losses. For example, a sudden disconnect during an active transaction in a network of ATM machines or other systems can cause uncertain states from which the end application may not recover, causing failure of the transaction. Thus, it is imperative to facilitate seamless handover of data so that information loss is minimized.

III-B Number of Backup Path

To prevent excessive resource usage for backup paths, and to meet the implicit service provider requirement of improving network resource utilization so as to increase the number of potential future demands that can be used

for protection, it is important to determine the appropriate number of backup paths to be shared.

When a failure occurs, up to k attempts will be made to find a backup path. If the k attempts fail, then the restoration attempt is considered to have failed and a new working path must be created for the customer. Thus, regardless of whether the restoration attempt succeeds, the system will spend T_r^k units of time trying to set up a backup path, where

$$\begin{aligned} E[T_r^k] &= pE[t] + 2(1-p)pE[t] + \cdots + (k-1)(1-p)^{k-2}pE[t] + k(1-p)^{k-1}E[t] \\ &= \frac{1-(1-p)^k}{p}E[t]. \end{aligned} \tag{4}$$

Suppose that as part of the SLA that a carrier has with the customer, there is an upper limit ϵ on the expected restoration time. This would be requested by a service class with shared backup protection (e.g. Silver class in Table 1). Thus the expected restoration time must satisfy

$$E[T_r^k] \leq \epsilon. \tag{5}$$

Substituting Eq. 4 into InEq. 5 results in

$$\frac{(1-(1-p)^k)}{p}E[t] \leq \epsilon. \tag{6}$$

The above InEq. can be expressed as

$$\frac{\ln(1-\frac{\epsilon}{E[t]}p)}{\ln(1-p)} \geq k \tag{7}$$

From InEq. 7, the maximum number of shared backup paths can be computed satisfying the requested restoration time of the service class.

For premium services, the network operator may also want to guarantee a certain probability of restoration success in the event of a failure. In other words, we may demand that the probability of restoration failure after k attempts does not exceed some limit, δ. So we require

$$P[\text{failure}] = (1-p)^k \leq \delta, \tag{8}$$

which implies that

$$k \geq \frac{\ln(\delta)}{\ln(1-p)}. \tag{9}$$

From InEq. 9, we can derive the minimum number of shared backup paths.

In accordance with the grade of service survivability, the carrier could determine the minimum or the maximum numbers of shared backup paths. If δ or ϵ is given according to the requested QoS, the other limit could be also determined such that

$$\frac{1-\delta}{p}E[t] \leq \epsilon, \qquad \text{equivalently} \qquad 1 - \frac{p\epsilon}{E[t]} \leq \delta. \tag{10}$$

Then, as soon as the QoS limits are determined, the carrier could restrict k to lie within a range of values given by

$$\frac{\ln(\delta)}{\ln(1-p)} \leq k \leq \frac{\ln(1-\frac{\epsilon}{E[t]}p)}{\ln(1-p)}. \tag{11}$$

As can be seen in Fig. 1, some carriers can refer the above range in accordance with the requested QoS for restoration time and recovery blocking rate. Normally, if the customers' traffic is so critical, then one would (to meet the SLA) assign a separate (or at least shared) backup path for this particular LSP. If the network is properly designed and used, the situation where no backup LSP is available, when the primary LSP fails, should not arise. In the event a new service request comes in and a backup cannot be found (and reserved) due to bandwidth exhaustion or for whatever reason, then the request (with protection LSP) should be denied. If the customer agrees to an unprotected LSP service, then depending upon the SLA, "best effort" service in the event of a node/link failure could be provided. If the unprotected LSP service cannot be provided also, then the request for this service is also denied, and depending upon the SLA only "best effort" service may be provided.

IV Path with Multiple Failures

The applications requesting high reliability, began to require a variety of failures to be taken into account. Among the failures, our analysis have focused on n-to-m protection with revertive mode [8] in GMPLS network since it is generally desirable that the alternate path can be switched back to the original working path once the failure is repaired in order to assure an optimized survivable network architecture. For this protection mode, we model and investigate both non-simultaneous and simultaneous ones for multiple path failures.

IV-A Signaling Procedure in GMPLS Network

In MPLS recovery, there are two modes, revertive and non-revertive. For revertive mode, traffic is automatically switched back from the recovery path to the original working path as soon as the working path recovers to a fault-free condition. In n-to-m protection, up to n working paths are protected using m protection paths which should be diversely routed. This analysis can also be applied to GMPLS protection where one of fundamentally most urgent needs is to increase the number of WDM channels considering today's growth rate of bandwidth demand. In our model, we assume that the following paths cannot be restored to another backup path for next fault before switching back to its original working path:

- The path which has been using a protection path since previous fault
- The path which is already in the restoration operation due to previous fault

For the two cases above, a higher-layer rerouting mechanism will be used to set up an alternate connection path. This approach is slower than the protection switching mechanism and so we use it only as a last resort. The procedure associated with the activation of a backup path is as follows:

Step 1 A fault occurs on a working path due to network impairment.
Step 2 GMPLS-based recovery mechanism detects the fault.
Step 3 *Failure Notify* message is sent to the node responsible for restoration.

Step 4 *if* a backup path is in use

then Perform rerouting function;

else Perform M:N protection function;

It is assumed that a mechanism for detecting and isolating multiple failures is in place in the network. In general, failures are detected by lower mechanisms. The lower mechanism passes up an alarm to an GMPLS control entity as soon as a node detects a failure. To do the analysis, we can use some of the theoretical framework developed in [9] for detecting and isolating multiple failures in WDM networks.

The above control steps could be implemented by Generalized RSVP signaling[4] as can be seen in Fig. 2. In Step 3, the node responsible for restoration, is either the ingress or the egress node, or both since our model is based on setting up backup path. The affected LSP and failed resources are identified in the *Failure Notify* message. As soon as the *Failure Notify* message is received, the responsible node checks if the precomputed backup path for the failed node, is already used, that is, the path with failure has not reverted to the original path. If the backup path is used, the rerouting function will be performed by requesting the path computation server in Fig. 2. While these steps are for revertive mode, the choice is dependent upon relative costs of the working and protection paths.

IV-B Blocking Probability for $M : N$ Protection with Revertive Mode

In this analysis, we will use the following assumptions:

- There are N backup paths and $M > N$ working paths in a $M : N$ protection domain.
- λ is the failure occurrence rate in a working path.
- The time for traffic to revert from a backup path to its original working path is exponentially distributed with rate μ.
- π_i is the steady state probability that i backup paths are used. In the state diagram (Fig. 4), state i corresponds to i backup paths being in use, and a transition from state i to state $i + 1$ occurs with rate $(N - i)\lambda$ for $i < m$.

Let n_f be the number of restoration requests by a failure occurrence upon a working path, n_r be the number of restoration completions (the number of accepted restoration requests), n_a be the number of restoration failures because the working path is already using a protection path, and n_b be the number of restoration failures because no backup path is available. It is clear that

$$n_f = n_r + n_a + n_b. \tag{12}$$

From the first assumption, the effective failure occurrence rate per working path can be defined as

$$\lambda_f = \frac{n_f - n_a}{n_f}\lambda. \tag{13}$$

This λ_f is used to determine the number of necessary backup paths, not λ. Let p_f be the restoration failure probability and p_f^* be the failure probability that excludes the blocked restoration requests due to using a protection path. We have

$$p_f = \frac{n_b}{n_f}, \qquad p_f^* = \frac{n_b}{n_f - n_a}. \tag{14}$$

If $p_f = p_f^*$ ($n_a = 0$) then the system can be described using the Erlang distribution, while $p_f \neq p_f^*$ ($n_a > 0$) leads to an Engset distribution. We derive the probability p_f^* from the state diagram in Fig. 4. For $1 \leq i \leq m$, from [7],

$$\begin{aligned} \pi_i &= \frac{(N-i+1)\lambda}{i\mu}\pi_{i-1} \\ &= \frac{\lambda^i \prod_{j=1}^{i}(N-j+1)}{i!\mu^i}\pi_0 \\ &= \binom{N}{i}\left(\frac{\lambda}{\mu}\right)^i \pi_0. \end{aligned} \tag{15}$$

Using the above Eq. 15 and the fact that $\pi_0 + \pi_1 + \cdots + \pi_m = 1$, the probability p_f^* can be expressed as

$$p_f^* = \pi_m = \frac{\binom{N}{m}\left(\frac{\lambda}{\mu}\right)^m}{\sum_{0 \leq i \leq m}\binom{N}{i}\left(\frac{\lambda}{\mu}\right)^i} \tag{16}$$

If the system does not consider the reversion, where the system can be described using the Erlang distribution, then we can compute $p_f = p_f^*$, which is the probability that an Erlang system with m states is in State m:

$$p_f = \pi_m = \frac{\rho^m/m!}{\sum_{n=0}^{m}\rho^n/n!}, \tag{17}$$

where $\rho = \lambda/\mu$.

For the above non-revertive mode in Eq. 17, depending on the configuration, the original working path may, upon being repaired, become the protection path, or it may be used for new working traffic. However, it is desirable to move the traffic to the original working path that is calculated based on network topology and network policies, gaining optimal network performance. Thus, we have more focused on the revertive mode developing expressions for some of the other probabilities related to the system in revertive mode.

Defining x to be the expected number of failures that occur while the working path is still using the protection path,

$$n_a = x n_r. \tag{18}$$

This follows from an examination of Fig. 3, which shows a scenario in which the interarrival time between failures is less than the average time required to allow traffic to revert to the original working path. From the figure we see that x is the mean number of failure events per restoration period. Because λ and μ are the respective failure

and restoration rates for the path, it follows that $x = \lambda/\mu$. We prove this below for the Markovian case. If the failure occurrences form a Poisson process with rate λ and the backup path holding times for each failure are exponentially distributed with mean $1/\mu$,

$$\begin{aligned} x &= \sum_{i=1}^{\infty} iPr[t_b \le t < t_b + t_i] \\ &= \sum_{i=1}^{\infty} i \int_{t=0}^{\infty} \int_{t_b=0}^{t} \int_{t_i=t-t_b}^{\infty} \mu e^{-\mu t} \frac{(\lambda t_b)^{i-1}}{(i-1)!} \lambda e^{-\lambda t_b} \lambda e^{-\lambda t_i} dt_i dt_b dt \\ &= \sum_{i=1}^{\infty} \frac{i\lambda^i \mu}{(\lambda+\mu)^{i+1}} \\ &= \frac{\lambda}{\mu}, \end{aligned} \tag{19}$$

where $t_b = t_0 + t_1 + t_2 + \cdots + t_{i-1}$ when i failures occur while the connection is using the backup path, as can be seen in Fig. 3.

Using Eq.s 12, 14, and 18, we obtain the following probabilities. The restoration failure probability, accounting for failures that occur while traffic is on a backup path, is

$$p_f = \frac{p_f^*}{1 + (1 - p_f^*)\frac{\lambda}{\mu}}. \tag{20}$$

The probability of restoration request acceptance can be computed as

$$\begin{aligned} p_r &= \frac{n_r}{n_f} \\ &= \frac{1 - p_f^*}{1 + (1 - p_f^*)\frac{\lambda}{\mu}}, \end{aligned} \tag{21}$$

and the probability of restoration failure resulting from using a protection path is found in a similar manner to be

$$\begin{aligned} p_a &= \frac{n_a}{n_f} \\ &= x p_r \\ &= \frac{(1 - p_f^*)\frac{\lambda}{\mu}}{1 + (1 - p_f^*)\frac{\lambda}{\mu}}. \end{aligned} \tag{22}$$

From the above Eq. 22, we can get the effective failure occurrence rate as

$$\begin{aligned} \lambda_f &= \lambda(1 - p_a) \\ &= \frac{\lambda}{1 + (1 - p_f^*)\frac{\lambda}{\mu}}. \end{aligned} \tag{23}$$

This effective failure occurrence rate is informative in utilizing backup LSPs, because most carriers prefer to make the LSP to revert back to its original working path. Usually, the routing of the protection path may not be as efficient as the original one. For this protection with revertive mode, the signaling steps in the section IV-A could be used.

IV-C Multiple Failures with Batch Arrivals

When a network operator creates protection groups with shared backup resources, it is important to maintain routing diversity among the various working paths in the group, so that a failure event (e.g. a fiber cut) impacts at most one working path. In practice it is not always possible to limit the effects of failure events in this way. If, for instance, several working paths in a restoration group pass through different switching offices that are in close proximity and they are all affected by a catastrophic event (e.g. a major earthquake) simultaneous failure of multiple working paths can occur.

Given the possibility of multiple failures, we need to develop a model that will allow us to determine the number of backup paths that are required in a protection group to guarantee that the probability of a working path's being unable to find a backup path is less than some maximum acceptable value. We first consider the case where we have a finite number of backup paths and an infinite number of working paths. We model multiple failures using batch arrivals, where the number of arrivals is a discrete random variable X whose probability mass function is $c_k = \mathsf{Pr}\{X = k\}$.

We model the restoration group as a set of N protection paths each with exponential restoration times where the average completion rate is μ. The rate of arrival of batches of failures amounting to k is $\lambda_k = c_k\lambda$. Considering that it is not desirable for paths with failures to wait till backup paths are available since fast restoration of service after a network failure is a crucial aspect of IP network. Thus, $M^X/M/N/N$ loss system[10] can be applied to this multiple failure model. An example of the state flow diagram for this model where $N = 3$ is shown in Fig. 5. The system of stationary balance equations that describe this system is

$$\begin{cases} 0 = -\lambda p_0 + \mu p_1 \\ 0 = -(\lambda + n\mu)p_n + (n+1)\mu p_{n+1} + \lambda \sum_{k=0}^{n-1} p_k c_{n-k}, \ n = 1, 2, \ldots, N-1 \\ 0 = -N\mu p_N + \lambda \sum_{k=0}^{N-1} \sum_{l=N-k}^{\infty} p_k c_l \end{cases} \tag{24}$$

We can get the state probabilities by using the approach given in [11], which is as follows. Recursively solving the balance equations gives

$$p_n = \frac{\lambda}{n\mu} \sum_{k=0}^{n-1} p_k C_{n-k}, \ n = 1, 2, \ldots, N, \tag{25}$$

where $C_j = \sum_{m=j}^{\infty} c_m = \mathsf{Pr}\{X \geq j\}$. By defining the sequence $\{g_n\}_{n=0}^{N}$ to be

$$g_n = \begin{cases} 1, & n = 0 \\ \frac{\lambda}{n\mu} \sum_{k=0}^{n-1} g_k C_{n-k}, & n = 1, 2, \ldots, N \end{cases} \tag{26}$$

we can express the state probabilities as

$$p_n = g_n p_0, \ n = 0, 1, 2, \ldots, N, \tag{27}$$

where $p_0 = \left[\sum_{n=0}^{N} g_n\right]^{-1}$.

The metric of interest in this case is the recovery blocking probability, i.e. restorability. To find the blocking probability for the $M^X/M/N/N$ system, we must compute

$$\begin{aligned} p_B &= \sum_{n=0}^{N} \mathsf{Pr}\left\{X > N-n | \text{System in State } n\right\} p_n \\ &= p_0 \sum_{n=0}^{N} \left(1 - \sum_{k=1}^{N-n} c_k\right) g_n \\ &= 1 - \frac{\sum_{n=0}^{N} \sum_{k=1}^{N-n} g_n c_k}{\sum_{n=0}^{N} g_n}. \end{aligned} \tag{28}$$

This is the probability that all the multiple failures of a batch will be unable to be completely restored, because there are more failure occurrences in the batch than there are backup paths available to restore them. In such a situation, at least one of the failures of the batch will have to be disregarded while the other failures are handled by restoration server. Alternatively, we can define a blocking metric that is simply the probability that the system in State N, which is the probability that no failure of a batch will be able to get handled. This is

$$p_N = \frac{g_N}{\sum_{n=0}^{N} g_n}. \tag{29}$$

We now plot these metrics using for the case where the batch size X has a geometric distribution. Thus $c_k = a(1-a)^{k-1}$, $0 < a \leq 1$, and the mean batch size is $1/a$. When $a = 1$, we have the $M/M/N/N$ system. For these examples, we have set $a = 0.9$, so that the probability that the batch size is greater than unity is 0.1. For the geometric distribution we can compute C_j as $C_j = \sum_{k=j}^{\infty} c_k = (1-a)^{j-1}$. Using this, we can determine the elements of the sequence g_n and obtain the state probabilities and the blocking probability metric for the system. For geometrically distributed bulk sizes, the blocking probability of a $M^X/M/N/N$ system is

$$p_B = \frac{\sum_{n=0}^{N} (1-a)^{N-n} g_n}{\sum_{n=0}^{N} g_n}. \tag{30}$$

This probability can be considered for restorability when some batches of failures occur on some working paths.

V Performance Evaluation

The performance of the proposed analytical model is analyzed by considering restoration failure rate, i.e. we characterize optical network services by restorability. It is assumed that a failure occurs with exponential distribution (mean is 10) and recovery time is 1(simulation time unit) in the simulation test. After setting up not

only 50(100 working paths in the other test) but 10 backup paths between ingress node and egress node, we generated failures over the working paths. Since these working paths are randomly chosen for each failure, some working paths could have multiple failures. It is assumed that all paths are pre-calculated and wavelengths are pre-assigned to working and backup paths.

Fig. 6 illustrates the impact of the multiple-failure effect comparing our model with the Erlang. In these graphs, $m = 10$ and two sets of curves are considered where one is $N = 50$ and the other is $N = 100$. The first graph in Fig. 6 indicates that our model is consistent with the simulation test. We observe that when N is small, the Erlang model is not appropriate to predict restoration failure probability (restorability) for a GMPLS network with a lower number of failures. As for the second graph, when the number of failures in a network is small, each working path with failures is likely to send current traffic on a backup path and the subsequent failures are unlikely to get the recovery service. Thus, effective failure occurrence rate per working path also becomes small. When N is large, it is more likely that a failure is unable to use a backup path because there is no free backup path.

We also investigated the performance varying the number of backup paths when the number of working paths is 10 and 100. In Figs. 7 and 8, we plot the recovery blocking probability (i.e. restoration failure probability) for $M : N$ protection groups with $N = 10$ and $N = 100$, respectively. Both probabilities are plotted versus the normalized utilization $N\rho$, and there is little difference in the plots where the number of backup paths are small. For a given number of backup paths, in order to have the restoration failure probability be less than some maximum allowable amount, we must have $N\rho$ less than some threshold, which can be determined from the graph. If we then increase the number of working paths in the protection group while keeping the number of backup paths fixed, we must make some additional adjustments to the network (such as reducing $1/\mu$, the average reversion time) in order to maintain the original level of performance. In this case, the required reduction in $1/\mu$ is proportional to the increase in the number of working paths.

In Fig. 9, we plot the value of the recovery blocking probability as defined in Eq. 28 and 30 versus ρ for various values of N. In Figs. 10 and 11, we respectively show similar plots for p_N as defined in Eq. 29 and for $p_B = p_N$ in the $M/M/N/N$ case which is non-revertive mode without batches of failures, as can be seen in Eq.17. These metrics are conservative because they assume an infinite pool of working paths. In reality, the number of working paths is limited and the probability that a bulk failure of a given size will occur is dependent on the number of remaining healthy working paths, and will decrease as the pool shrinks.

In examining these plots, we note that there is very little difference in the values obtained for p_B as defined in Eq. 28 versus p_N as defined in Eq. 29, except for very rare failure (the values of ρ that are very close to zero). This is because we have defined p_B as the probability that the next arriving batch of failures is unable to be completely restored, which for $\rho = 0$ is the probability that $X > N$. For most values of ρ, we obtain a slightly more conservative metric by using Eq. 28.

Using these plots, it is possible to determine the number of backup paths that will guarantee a desired maximum

restorability for a failed working path that not be switched over. For instance, if failure events occur at an average rate of once every day (with 1/10 failure events involving multiple failed working paths) while repairs to failed working paths take half a day on average (giving $\rho = 0.5$), a blocking probability of at most 10^{-6} can be guaranteed if the protection group contains at least 9 backup paths.

When we compare Figs. 9 and 10 to Fig. 11 which shows p_N for the case where multiple simultaneous failures never occur, we see that there is little difference in performance between the two systems for small values of N, although the gap between the two metrics increases with decreasing values of ρ. But, the gap between the metrics for the two systems increases with increasing N; for $N = 20$ the difference is roughly one order of magnitude. Thus, determining bulk arrival statistics becomes an issue when recovery is slow relative to the rate of failures yet a high level of reliability is required. Even in the event of natural disasters, some traffic with very high level of reliability has to be handled by enough backup paths. In many cases, some carriers should borrow the enough backup resources from the other carriers to get the enough backup resources avoiding the same region of failure as working paths [2]. Therefore, our analysis will make carriers provision backup paths efficiently in terms of resource utilization.

VI Conclusion

In this paper, we prooposed a new analytical model for shared backup path provisioning in GMPLS networks. In our model, protection bandwidth capacity was considered as the main cost of recovery QoS, with the result that different amount of backup resources could be assigned to services with different levels of protection. We have also discussed some of the issues associated with provisioning shared backup paths in networks that use GMPLS as part of their control plane. We have reviewed some of the ways that GMPLS, in combination with other QoS mechanisms, can be used to allow service providers to offer customized levels of protection to their customers. To determine the optimum size of a $M : N$ protection group given QoS constraints, we have developed a model that predicts the amount of time required to establish a backup path. We have also developed models for $M : N$ protection with reversion for both single failures and batches of mutiple failures which are modeled by a $M^X/M/N/N$ system. The examination of our simulation results demonstrated that shared protection groups can be sized so that the probability that a backup path is unavailable is less than a desired threshold. The results also showed that when multiple simultaneous failures are rare, the single failure model is a good approximation that can be used for protection group sizing.

Finally, future work is to expand on this work by analyzing the effect of network topology on the probability of multiple failure events and by studying switchover delays in more detail. In particular, we are examining the behavior of several restoration signaling algorithms in a variety of failure scenarios.

References

[1] O. Gerstel and R. Ramaswami, "Optical Layer Survivability: A Services Perspective", *IEEE Communications Magazine*, vol. 38, no. 3, pp. 104-113, March 2000.

[2] H. Ishimatsu et al., "Carrier Needs Regarding Survivability and Maintenance for Switched Optical Networks", *Internet draft*, draft-hayata-ipo-carrier-needs-00.txt, Nov. 2000.

[3] P. Smith, et al, "Generalized MPLS - signaling functional description", *Internet Draft*, draft-ietf-mpls-generalized-mpls-signaling-07.txt, Nov. 2001.

[4] P. Smith, et al, "Generalized MPLS Signaling - RSVP-TE Extensions", *Internet Draft*, draft-ietf-mpls-generalized-rsvp-te-06.txt, Nov. 2001.

[5] P. Smith, et al, "Generalized MPLS Signaling - CR-LDP Extensions", *Internet Draft*, draft-ietf-mpls-generalized-cr-ldp-01.txt, Mar. 2001.

[6] Many, "OIF UNI Signaling Specification", OIF2000.125.3, Feb. 2001.

[7] L. Kleinlock, "Queueing Systems: Theory, vol.I", *John Wiley & Sons*, NewYork, 1975.

[8] V. Sharmai et al, "Framework for MPLS-based Recovery", *IETF Draft*, draft-ietf-mpls-recovery-frmwrk-02.txt, Mar. 2001.

[9] C. Mas and P. Thiran, "An Efficient Algorithm for Locating Soft and Hard Failures in WDM Networks", *The IEEE Journal of Selected Areas in Communications*, vol. 18, no. 10, pp. 1900-1911, October, 2000.

[10] M. L. Chaudhry and J. G. C. Templeton, "A First Course in Bulk Queues", *John Wiley & Sons, Inc.*, 1983.

[11] I. W. Kabak, "Blocking and Delays in $M^{(x)}/M/c$ Bulk Arrival Queueing Systems", *Management Science*, vol. 17, pp. 112-115, 1970.

Table 1: Protection level example

Service level	Protection plan
Gold	Dedicated protection: $1+1$, $1:1$
Silver	Shared protection: $M:N$, $1:n$
Bronze	Rerouting

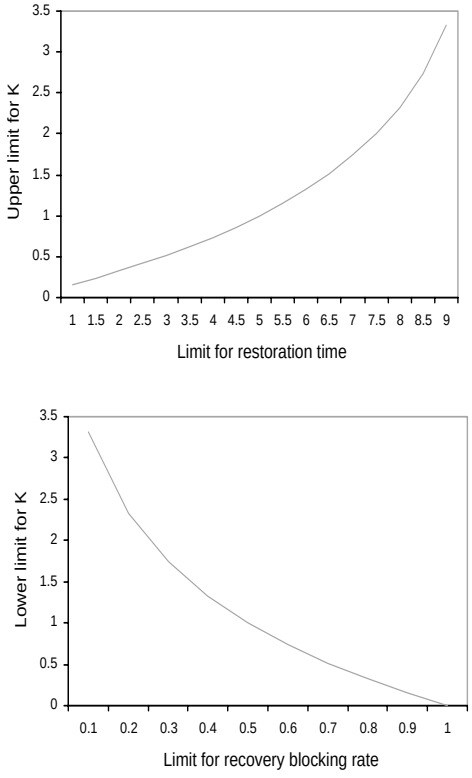


Figure 1: Range for the number of backup paths

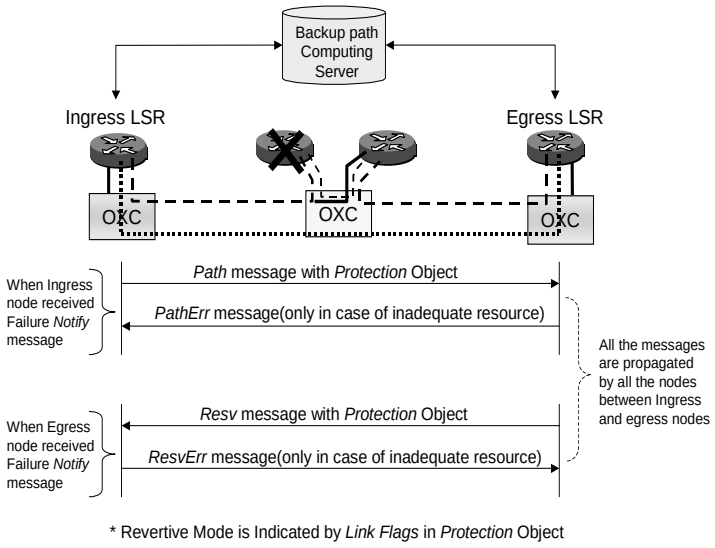


Figure 2: GMPLS signaling system

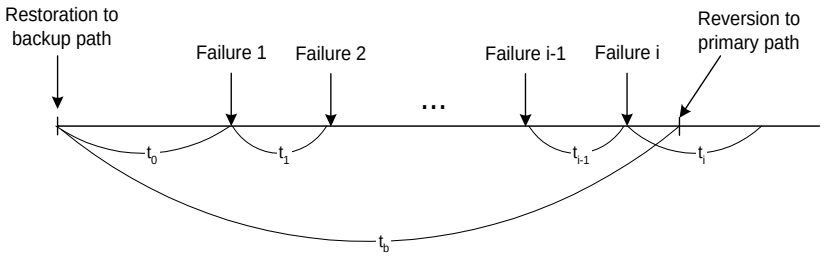


Figure 3: Time model for multiple failures

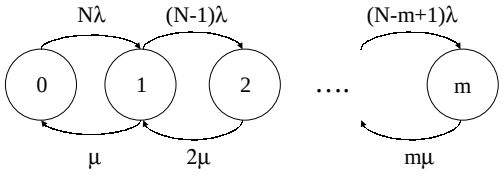


Figure 4: State diagram for multiple failures

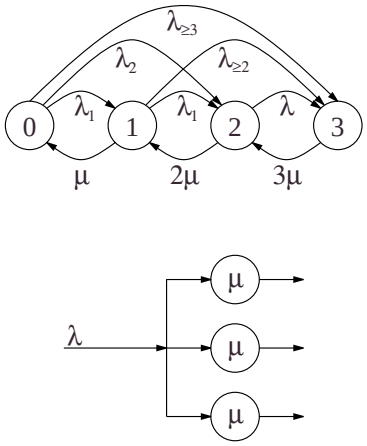
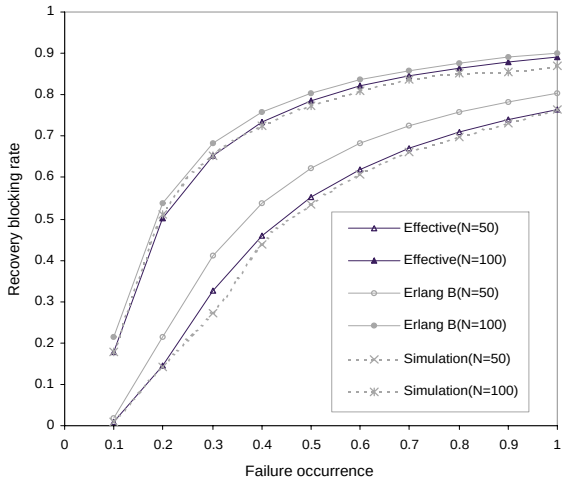


Figure 5: Sketch and state diagram for $M^X/M/3/3$ system (no buffering). The rates of the form $\lambda_{\geq k}$ denote arrival rates of groups with size of at least k. Thus, for example, $\lambda_{\geq 2} = \lambda \sum_{n=2}^{\infty} c_n = \lambda(1 - c_1)$.



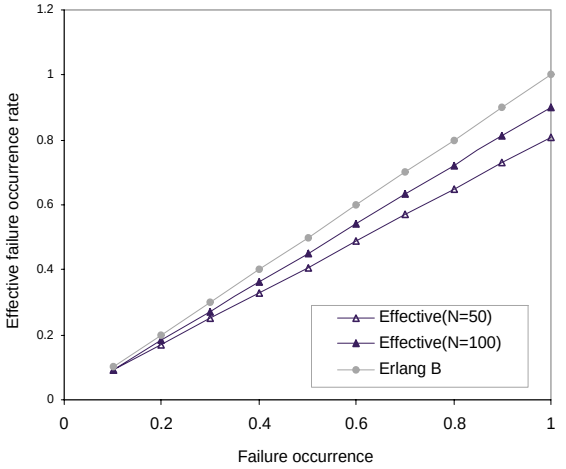


Figure 6: Impact of multiple failures

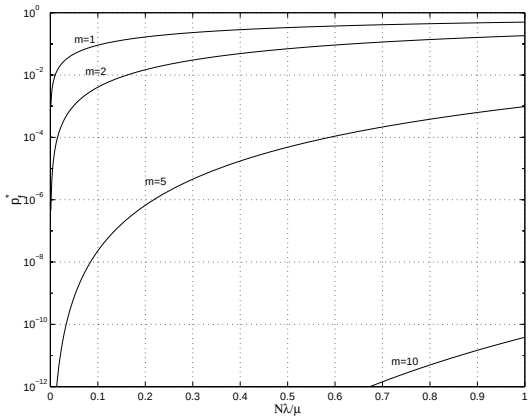


Figure 7: Recovery blocking probability for revertive mode with $N = 10$ under various values of m.

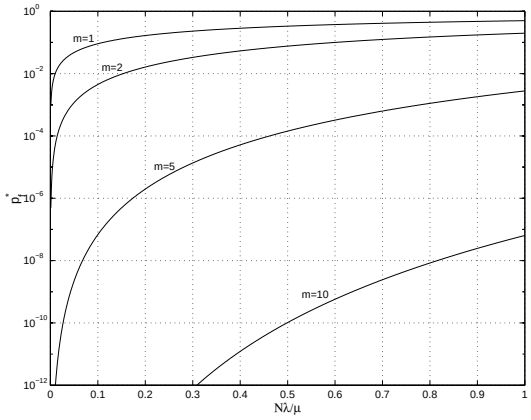


Figure 8: Recovery blocking probability for revertive mode with $N = 100$ under various values of m.

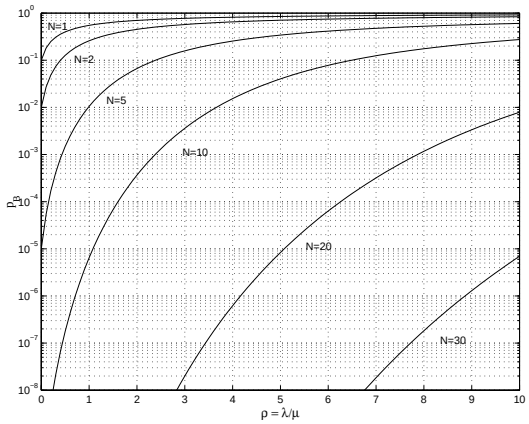


Figure 9: Probability that all the failures of a batch cannot be restored, versus utilization ($\mathsf{Pr}\{X > 1\} = 0.1$)

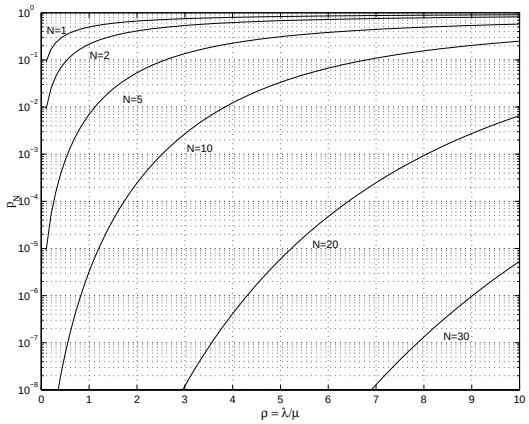


Figure 10: Probability that no failure of a batch can be restored, versus utilization ($\mathsf{Pr}\{X > 1\} = 0.1$)

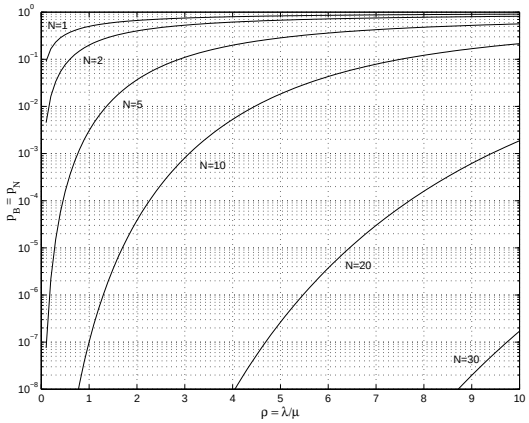


Figure 11: Recovery blocking probability for non-revertive mode with single arrivals only, versus utilization.